UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/712,398	11/14/2000	Scott C. Harris	BIODONGLE/SCH	8991

23844   7590   02/23/2004

SCOTT C HARRIS
P O BOX 927649
SAN DIEGO, CA 92192

EXAMINER
MAHMOUDI, HASSAN

ART UNIT	PAPER NUMBER
2175	

DATE MAILED: 02/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cov r she t with th correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _05 December 2003_.
2a) ☐ This action is FINAL.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-21_ is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _1-21_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some * c) ☐ None of:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. _____.
    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
       application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 05-December-2003, the specification of the disclosure and claims 2-3, 8-9, 15, and 18-20 are amended per applicant's request. Claims 1-21 are presently pending in the application.

2. Upon further search in view of the amended claims, previously objected to claims for containing "allowable subject matter" (claims 18 and 20, now written as independent claims), are rejected under a new 35 U.S.C. 103(a) rejection. Therefore, this Office Action is made "non-final" in view of the new grounds of rejection.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-2, 6-7, and 15-17 are rejected under 35 U.S.C. 102(e) as being anticipated by

Applebaum (U.S. Publication No. 2002/0044655.)

As to claim 1, Applebaum teaches a method (see Abstract), comprising:

storing encrypted information associated with a computer program (see paragraph 0009,

where "storing encrypted information" is read on "encryption methods using symmetric and

asymmetric keys provide a mechanism for securing data stored on the information

appliance", and see paragraphs 0040-0041, where "computer program" is read on

"application". Also see paragraphs 0034 and 0042, where it is taught that "the entire

information file" is "encrypted" and "stored" within the information appliance);

obtaining personal information as part of a startup sequence for the computer program

(see Abstract, and see paragraphs 0052 and 0056); and

reading the encrypted information (see figure 8), decrypting information contained

therein to obtain decrypted information (see paragraph 0022), and comparing the personal

information with the decrypted information (see paragraph 0052, and see page 9, claim 42);

and allowing the computer program to run normally only if the personal information agrees

with the decrypted information in a specified way (see pages 8-9, claim 36, where "allowing

the computer program to run normally" is read on "allowing access to the distributed

productivity environment".)

As to claim 2, Applebaum teaches wherein the personal information is biometric

information (see Abstract), and the comparing comprises comparing the biometric

information with other biometric information in the encrypted information (see paragraph

0052.)

As to claim 6, Applebaum teaches the method further comprising determining if a

biometric reader is attached to a port (see paragraph 0048), and wherein the program is only

allowed to run if the biometric reader is attached to the port (see paragraph 0047.)

As to claim 7, Applebaum teaches the method further comprising allowing the software

to run in a limited exception mode without establishing that the personal information agrees

with the decrypted information (see pages 8-9, claim 36.)

As to claim 15, Applebaum teaches a system (see Abstract, and see paragraph 0008),

comprising:

a computer (see figures 10 and 11, and see paragraphs 0043 and 0048), running an

operating system (see paragraph 0039), which includes an ability to run a program (see

paragraph 0041);

at least one port, associated with the computer, the port capable of receiving at least one

peripheral device thereon (see figure 11, and see paragraphs 0047-0048, and 0050); and

a user interface, associated with the computer (see paragraph 0052), receiving a

command to run a specified program, and operating to decrypt encrypted reference biometric

information associated with the specified program (see paragraphs 0022, and 0041-0042), to

compare currently-obtained biometric information with the reference biometric information

(see paragraph 0042), and which allows the program to run in a specified way only when the currently-obtained biometric information matches the reference biometric information (see pages 8-9, claim 36, where "allowing the computer program to run normally" is read on "allowing access to the distributed productivity environment".)

As to claim 16, <u>Applebaum</u> teaches wherein the operating system operates to first detect whether a biometric reading device is attached to the port (see paragraph 0048), and then detect whether biometric information has been received from the biometric reading device, the program being allowed to run in the specified way only when both the biometric reading device is attached, and biometric information which is received matches the reference biometric information (see paragraphs 0048 and 0052.)

As to claim 17, <u>Applebaum</u> teaches wherein the operating system decrypts the reference biometric information (see paragraph 0022.)

5. Claims 8-14, 19 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by <u>Brody</u> (U.S. Publication No. 2001/0051928.)

   As to claim 8, <u>Brody</u> teaches a method (see Abstract), comprising:

   requesting a computer system to install a specified computer program (see figure 3, and see paragraphs 0063 and 0082);

determining whether the computer program is verified for installation (see paragraph 0023);

obtaining a reference biometric information from an authorized user (see paragraph 0094) at the time of installing the software (see Abstract), responsive to the determining that the computer program is verified for installation (see paragraphs 0006, 0082, and 0092); and thereafter allowing the program to run normally only when biometric information is obtained which matches the reference biometric information (see paragraph 0153.)

As to claim 9, <u>Brody</u> teaches the determining comprises determining if a specified license used for the installation has already been used for another installation (see paragraphs 0023, and 0058-0060.)

As to claim 10, <u>Brody</u> teaches wherein the determining uses a specified unique code that was distributed with the program, and determines from a server whether the unique code has already been used for an installation (see paragraphs 0010, 0015, 0019, and 183.)

As to claim 11, <u>Brody</u> teaches the method further comprising, after determining that the installation is authorized, sending the reference biometric information to a server (see paragraph 0098.)

As to claim 12, <u>Brody</u> teaches the method further comprising, at the server, encrypting the reference biometric information (see paragraph 0152), and returning encrypted biometric

reference information which is stored with the program, and which is used by the allowing

(see page 23, claim 9, where "biometric reference information" is read on "personalization"

and "stored within the program" is read on "within the information stream".)

As to claim 13, Brody teaches wherein the allowing retrieves encrypted biometric

information (see page 23, claim 9), decrypts the biometric information (see paragraph 152),

and allows the program to run normally only if the decrypted biometric information matches

a currently entered biometric information (see paragraph 0153.)

As to claim 14, Brody teaches wherein the reference biometric information is encrypted

at the server using a private key of a public key-private key pair, and the reference biometric

information is decrypted when software is to be run, using the public key corresponding to

the private key (see paragraph 0152.)

As to claim 19, Brody teaches a computer readable media (see paragraph 0062),

containing instructions (see paragraph 0083) causing the computer to:

detect a request to run a specified already-installed program (see figure 3, and see

paragraphs 0023, 0039, 0063 and 0082);

obtain current biometric information (see paragraph 0094);

decrypt an encrypted reference information including reference biometric information

therein, and obtaining reference biometric information therefrom (see paragraph 0152);

compare the reference biometric information with the current biometric information (see

paragraph 0153); and

allow the specified program to run into specified way only when the reference biometric

information matches the current biometric information (see paragraph 0153.)

As to claim 21, <u>Brody</u> teaches wherein the specified way is an unrestricted run which

does not detect a number of other executions or operations of the program (see paragraphs

0097 and 0099.)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

7. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Applebaum</u> (U.S.

Publication No. 2002/0044655) in view of <u>Brody</u> (U.S. Publication No. 2001/0051928.)

As to claim 3, <u>Applebaum</u> teaches the method further comprising encrypting the

biometric code at the server (see paragraph 0009) and returning an encrypted sequence to the

computer program as the encrypted information (see figure 4, and see paragraph 0018.)

<u>Applebaum</u> does not teach installing the computer program by entering a biometric code,

sending the biometric code to a server.

Brody teaches a method of personalizing published software (see Abstract), in which he

teaches installing the computer program by entering a biometric code, sending the biometric

code to a server (see figure 2, and see paragraph 147.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Applebaum to include installing the computer

program by entering a biometric code, sending the biometric code to a server.

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Applebaum by the teaching of Brody, because

installing the computer program by entering a biometric code, sending the biometric code to

a server, would offer personalized installation of the software for remoter clients within a

distributed network/system.

As to claim 4, Applebaum as modified teaches wherein the encrypting uses a private key

at the server (see Applebaum, paragraph 0042), and the decrypting verifies a signature of the

private key (see Applebaum, paragraph 0052.)

As to claim 5, Applebaum as modified teaches wherein the encrypting uses a private key

at the server (see Applebaum, paragraph 0042), and the decrypting uses a public key included

as a part of the computer program (see Applebaum, paragraph 0042, and see page 7, claim

20.)

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Applebaum</u> (U.S.

Publication No. 2002/0044655) in view of <u>Shinzaki</u> (U.S. Publication No. 2003/0005310.)

As to claim 18, <u>Applebaum</u> teaches a system (see Abstract, and see paragraph 0008),

comprising:

a computer (see figures 10 and 11, and see paragraphs 0043 and 0048), running an

operating system (see paragraph 0039), which includes an ability to run a program (see

paragraph 0041);

at least one port, associated with the computer, the port capable of receiving at least one

peripheral device thereon (see figure 11, and see paragraphs 0047-0048, and 0050); and

a user interface, associated with the computer (see paragraph 0052), receiving a

command to run a specified program, and operating to decrypt encrypted reference biometric

information associated with the specified program (see paragraphs 0022, and 0041-0042), to

compare currently-obtained biometric information with the reference biometric information

(see paragraph 0042), and which allows the program to run in a specified way only when the

currently-obtained biometric information matches the reference biometric information (see

pages 8-9, claim 36, where "allowing the computer program to run normally" is read on

"allowing access to the distributed productivity environment"); and

wherein the operating system decrypts the reference biometric information (see paragraph

0022.)

<u>Applebaum</u> does not teach:

wherein the operating system determines a time and current biometric information is obtained, and compares the time with the current time, and allows the program to run in the specified way only when the time is within a specified interval of the current time.

Shinzaki teaches a user verification system (see Abstract), in which he teaches wherein the operating system determines a time and current biometric information is obtained (see paragraph 0029, where "determining a time and current biometric information is obtained" is read on "the time stamp" when "the biometric feature data" has been "extracted"), and compares the time with the current time (see paragraph 0029, "comparing the original time stamp" with "the current time" is taught), and allows the program to run in the specified way only when the time is within a specified interval of the current time (see paragraph 0029, where "the current time falls within a predetermined range" is taught, also see paragraphs 0048, 0058, 0071, and 0083.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Applebaum to include wherein the operating system determines a time and current biometric information is obtained, and compares the time with the current time, and allows the program to run in the specified way only when the time is within a specified interval of the current time.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Applebaum by the teachings of Shinzaki, because including wherein the operating system determines a time and current biometric information is obtained, and compares the time with the current time, and allows the program to run in the specified way only when the time is within a specified interval of the current time, would

allow the system to perform certain tasks within certain pre-determined time intervals, as established at the time the biometric data was obtained and/or retrieved by the system. The specific tasks could include, but not be limited to, identification of the user, as taught by Shinzaki (see paragraphs 0029 and 0058.)

9. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brody (U.S. Publication No. 2001/0051928) in view of Shinzaki (U.S. Publication No. 2003/0005310.)

As to claim 20, Brody teaches a computer readable media (see paragraph 0062), containing instructions (see paragraph 0083) causing the computer to:

detect a request to run a specified already-installed program (see figure 3, and see paragraphs 0023, 0039, 0063 and 0082);

obtain current biometric information (see paragraph 0094);

decrypt an encrypted reference information including reference biometric information therein, and obtaining reference biometric information therefrom (see paragraph 0152);

compare the reference biometric information with the current biometric information (see paragraph 0153); and

allow the specified program to run into specified way only when the reference biometric information matches the current biometric information (see paragraph 0153.)

Brody does not teach:

wherein the compares also compares a time and current biometric information was obtained with a current time, and allows the specified program to run in the specified way only when the time is within a specified interval of the current time.

Shinzaki teaches a user verification system (see Abstract), in which he teaches wherein

the compares also compares a time and current biometric information was obtained with a

current time (see paragraph 0029, "comparing the original time stamp" with "the current

time" is taught), and allows the specified program to run in the specified way only when the

time is within a specified interval of the current time (see paragraph 0029, where "the current

time falls within a predetermined range" is taught, also see paragraphs 0048, 0058, 0071, and

0083.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Brody to include wherein the compares also

compares a time and current biometric information was obtained with a current time, and

allows the specified program to run in the specified way only when the time is within a

specified interval of the current time.

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Brody by the teachings of Shinzaki, because including

wherein the compares also compares a time and current biometric information was obtained

with a current time, and allows the specified program to run in the specified way only when

the time is within a specified interval of the current time, would allow the system to perform

certain tasks within certain pre-determined time intervals, as established at the time the

biometric data was obtained and/or retrieved by the system. The specific tasks could include,

but not be limited to, identification of the user, as taught by Shinzaki (see paragraphs 0029

and 0058.)

Response to Arguments

10. Applicant's arguments filed on 05-December-2003 with respect to the rejected claims in view of the cited references have been fully considered but they are moot in view of the new grounds for rejection.
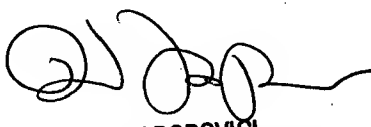
Conclusion

11. Any inquiries concerning this communication or earlier communications from the examiner should be directed to Tony Mahmoudi whose telephone number is (703) 305-4887. The examiner can normally be reached on Mondays-Fridays from 08:00 am to 04:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici, can be reached at (703) 305-3830.

tm

February 16, 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100